



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/398,914	09/16/1999	NED HOFFMAN	STA-21	1647

20575 7590 12/09/2002

MARGER JOHNSON & MCCOLLOM PC  
1030 SW MORRISON STREET  
PORTLAND, OR 97205

EXAMINER

REAGAN, JAMES A

ART UNIT PAPER NUMBER

3621

DATE MAILED: 12/09/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/398,914

Applicant(s)

HOFFMAN ET AL.

Examiner

James A. Reagan

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 September 2002.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-51 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-51 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 September 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 11.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

**DETAILED ACTION**

**Status of Claims**

1. This action is in response to the amendment received on 26 September 2002.
2. Claims 1, 20, and 25 have been amended (paper #10).
3. Claims 1-51 have been examined.
4. The rejections of claims 1, 20, and 25 have been updated to reflect the amended limitations.
5. The rejections of claims 2-19, 21-24, and 26-51 are unchanged.

**Information Disclosure Statement**

6. The Information Disclosure Statement filed on 26 September 2002 (paper no. 11) has been considered. An initialed copy of the Form 1449 is enclosed herewith.

**Specification**

7. The objection to the specification contained within the previous Office action is withdrawn. Examiner thanks the Applicant for updating and correcting the minor deficiencies in the specification.

### RESPONSE TO ARGUMENTS

8. Applicant's arguments received on 26 September 2002 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

With regard to the limitations of claims 1, 20, and 25, Applicant argues the difference between authentication and identification. Although the Applicant himself makes a clear distinction between authentication and identification, and asserts that the claimed invention performs identification and not authentication, this nuance is not clearly and distinctly brought out in the claim language. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., identification in lieu of authentication) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Bianco discloses

identification practices (see column 2, line 66 to column 3, line 2). Although Applicant asserts that identification and authentication are separate and distinct functions in the electronic security arts, the Examiner disagrees. Microsoft Computer Dictionary defines authentication as follows:

**Authentication** *n.* In a multiuser or network operating system, the process by which the system validates a user's logon information. A user's name and password are compared against an authorized list, and if the system detects a match, access is granted to the extent specified in the permission list for that user.<sup>1</sup>

Clearly, one way of authenticating a user ID and password is to compare them to a list, as was asserted by the Applicant in the arguments. In reality, there are many equivalent techniques of granting access to a user, the process being merely one of design choice. It would have been necessary to one of ordinary skill in the art at the time of the invention to provide an authentication step to properly identify each user with the system. As shown in the definition above, granting access only to properly authorized persons allows access to a specified extent (rules) according to their permission right. As shown, identification and authorization are nearly synonymous within the electronic security arts.

Applicant also argues that Bianco does not disclose a rules module that is "user-customized means having been customized by or for a user." Examiner disagrees and points to column 18, lines 18-26. Bianco clearly discloses

---

<sup>1</sup> Microsoft Computer Dictionary (4<sup>th</sup> ed.). © 1999 Microsoft Corporation. Redmond, Washington.

biometric policies, which are inherently set either by a user who is setting up his account or by a system administrator who defines access rights to a system depending on the level of permission granted. Clearly, if a user (primary or subordinate) is associated with a particular policy, the user is held to the rules of that policy.

9. The following is a **Final Rejection** of all claims and associated limitations pending in the current application as amended in paper #7.

**Examiner's note:** Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the *entire* reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

### **Claim Rejections - 35 USC § 102**

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

**NOTE:** The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

11. Claims 1-26, 30-33, 36-37, 39, 41, 43-46, 49 & 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Bianco et al (U.S. Patent No. 6,256,737).

In re claims 1 Bianco et al. shows in figures 1-34 and related text a tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, an electronic identifier and an electronic rule module clearinghouse, said method comprising the steps of: a user registration step wherein a user registers with an electronic identifier at least one registration sample (column 10, lines 7 – 13); the formation of a rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data (accounting group) (wherein it is noted that page 37, line 8 of the instant application defines a pattern data to include the user's company division), of a user is associated with at least one execution command (access group of resources) of the user (column 2, lines 53-66; column 18, lines 8 – 17); a user identification step, wherein the electronic indicator compares bid biometric sample taken directly from the person of the user with at least one previously

registered biometric sample for producing either a successful or failed identification of the user (column 8, lines 14 - 21); a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission (column 8, lines 19 -21; column 24, lines 53-56); wherein a biometrically authorized electronic transmission is conducted without the user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipes (column 7, lines 47 - 67). With regard to the limitation of authenticating a user, there are many equivalent techniques of granting access to a user, the process being merely one of design choice. As shown in the definition above, granting access only to properly authorized persons allows access to a specified extent (rules) according to their permission right. As shown, identification and authorization are nearly synonymous within the electronic security arts. With regard to the limitation of a rules module that is "user-customized means having been customized by or for a user," Bianco clearly discloses biometric policies (column 18, lines 18-26), which are inherently set either by a user who is setting up his account or by a system administrator who defines access rights to a system depending on the level of permission granted. Clearly, if a user (primary or subordinate) is associated with a particular policy, the user is held to the rules of that policy.

In re claim 2 Bianco et al. shows in figures 1-34 and related text the electronic rule module clearinghouse communicates with one or more third-party computers (Fig.1).

In re claim 3 Bianco et al. shows in figures 1-34 and related text any of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the users rule modules, presentation of electronic data customized to the user's rue modules (column 1, lines 8-29).

In re claim 4 Bianco et al. shows in figures 1-34 and related text wherein the pattern data comprises any of the following; a user unique identification code, demographic information; an email address, a financial account, a secondary biometric, internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchase patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an internet protocol address, a digital signature, an encryption key, and instant messaging address, personal medical records, an electronic audio signature, an electronic visual signature (column 54, lines 52 – 57).

In re claim 5 Bianco et al. shows in figures 1-34 and related text pattern data (group) for a user is provided for the rule module by any of he following the

user, the electronic rule module clearinghouse, or an authorized third party (column 19, lines 13-17).

In re claim 6 Bianco et al. shows in figures 1-34 and related text an execution command (group of resources that each member will need to access) for a user is provided for the rule module by any of the following: the user, the electronic rule module clearinghouse, or an authorized third party (column 19, lines 13-17).

In re claim 7 Bianco et al. shows in figures 1-34 and related text a user re-registration check step, wherein the user's registration biometric sample is compared against previously registered biometric samples wherein if a match occurs, the computer system is alerted to the fact that the user has attempted to re-register with the electronic identifier (column 29, lines 4-10).

In re claim 8 Bianco et al. shows in figures 1-34 and related text any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print (column 7, lines 59-67).

In re claim 9 Bianco et al. shows in figures 1-34 and related text during the identification step the user provides a personal identification code to the electronic identifier along with a biometric sample for the purposes of identifying the user (column 23, lines 31 - 33).

In re claim 10 Bianco et al. shows in figures 1-34 and related text a biometric theft resolution step, wherein a user's personal identification code is

changed when the user's biometric sample is determined to have been fraudulently duplicated (column 28, line 60 – column 29, line 39).

In re claim 11 Bianco et al. shows in figures 1-34 and related text execution of an execution command authorizes the user to access stored electronic data (column 1, lines 7-17).

In re claim 12 Bianco et al. shows in figures 1-34 and related text accessing stored electronic data results in activation of an Internet-connected device (column 1, lines 15 – 29).

In re claim 13 Bianco et al. shows in figures 1-34 and related text an execution command processes electronic data to provide the user with a requested electronic transmission (column 54, lines 52-56).

In re claim 14 Bianco et al. shows, in figures 1-34 and related text, processing comprises invoking the following; a user's digital certificate, a user's identity scrambler, a user's interactive electronic consumer loyalty or consumer rewards program, a user's interactive electronic advertising, a user's interactive instant messaging program, a user's email authentication, and an automated electronic intelligent agent for electronic data search and retrieval that is customized to the user's requests (column 54, lines 52-56).

In re claim 15 Bianco et al. shows, in figures 1-34 and related text an execution command presents electronic data that is customized to the user's retested electronic transmission (column 2, lines 1-13). Where it is noted in this

example that e-mail received by a user is commonly known in the art to be customized to the user.

In re claim 16 Bianco et al. shows, in figures 1-34 and related text a user log-in repeat step, wherein during an electronic transmission the user is periodically required by the electronic identicator to present the user's bid biometric sample or at least one of the user's pattern data (column 30, lines 15-29).

In re claim 17 Bianco et al. shows, in figures 1-34 and related text, a communications step wherein any if the following is used: the internet, an intranet, an extranet, a local area network, a wide area network (column 2, lines 1 – 13).

In re claim 18 Bianco et al. shows, in figures 1-34 and related text a third party registration step wherein a third-party registers identification data with the electronic identicator, the identification data comprising any of the following; a biometric, a digital certificate, an Internet protocol address, or a biometric input apparatus hardware identification code (column 18, lines 50-64).

In re claim 19 Bianco et al. shows, in figures 1-34 and related text a third party identification step, wherein a third-party providing the user with electronic transmissions is identified by the electronic identicator by comparing the third-party's bid identification data with the third-party's registered identification data (column 18, lines 50-64).

In re claim 20 Bianco et al. shows, in figures 1-34 and related text, a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identifier; wherein a user registers with an electronic identifier at least one registration biometric sample taken directly from the person of the user (column 10, lines 7 – 13); an electronic rule module clearinghouse, having at least one rule module further comprising at least one pattern data of a user associated with at least one execution command of the user, for executing at least one electronic transmission (column 2, lines 53-66; column 18, lines 8 – 17); an electronic identifier, for comparing the bid biometric sample with registered biometric samples of users (column 8, lines 14 - 21); a command execution module for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission (column 8, lines 19 –21; column 24, lines 53-56); wherein no man-made memory tokens such as smartcards, or magnetic swipe cards are presented by the user to conduct the electronic transmission (column 7, lines 47 – 67). With regard to the limitation of authenticating a user, there are many equivalent techniques of granting access to a user, the process being merely one of design choice. As shown in the definition above, granting access only to properly authorized persons allows access to a specified extent (rules) according to their permission right. As shown, identification and authorization are nearly synonymous within the electronic security arts. With regard to the limitation of a rules module that is “user-customized means having

been customized by or for a user," Bianco clearly discloses biometric policies (column 18, lines 18-26), which are inherently set either by a user who is setting up his account or by a system administrator who defines access rights to a system depending on the level of permission granted. Clearly, if a user (primary or subordinate) is associated with a particular policy, the user is held to the rules of that policy.

In re claim 21 Bianco et al. shows, in figures 1-34 and related text the command module communicates with one or more third-party computers (column 24, lines 53-56; column 1, lines 15 – column 2, lines 17).

In re claim 22 Bianco et al. shows, in figures 1-34 and related text the pattern data comprises any of the following; a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, and electronic audio signature, and an electronic visual signature (column 54, lines 52 –57).

In re claim 23 Bianco et al. shows, in figures 1-34 and related text pattern data for the user is provided for the rule module by any of the following; the user,

the electronic rule module clearinghouse, or an authorized third party (column 19, lines 13-17).

In re claim 24 Bianco et al. shows, in figures 1-34 and related text an execution command for a user is provided for the rule module by any of the following the user, the electronic rule module clearinghouse, or an authorized third party (column 19, lines 13-17).

In re claim 25 Bianco et al. shows in figures 1-34 and related text a primary and subordinated user registration step wherein a primary and subordinated user each register with an electronic identifier at least one registration biometric sample taken directly from the person of the a primary and subordinated user (column 10, lines 7-13; column 49, lines 8-65); the formation of a rule module customized to a primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the a primary and subordinated user is associated with at least one execution command of the a primary and subordinated user (column 2, lines 53-66; column 18, lines 8 – 17; column 49, lines 8-65); a subordinated user identification step, wherein the electronic indicator compares a bid biometric sample taken directly from the person of the subordinated user with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user (column 8, lines 14 – 21; column 49, lines 8-65); a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of

the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules (column 49, lines 8-65); a command execution step, wherein upon successful identification of the subordinated user and determination that at least one of the primary user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the user is invoked to execute at least one electronic transmission (column 8, lines 19 –21; column 24, lines 53-56; column 49, lines 8-65); wherein a biometrically authorized electronic transmission is conducted without the user presenting any personalized man-made memory tokens such as smartcards, or magnetic swipes (column 7, lines 47 – 67). With regard to the limitation of authenticating a user, there are many equivalent techniques of granting access to a user, the process being merely one of design choice. As shown in the definition above, granting access only to properly authorized persons allows access to a specified extent (rules) according to their permission right. As shown, identification and authorization are nearly synonymous within the electronic security arts. With regard to the limitation of a rules module that is "user-customized means having been customized by or for a user," Bianco clearly discloses biometric policies (column 18, lines 18-26), which are inherently set either by a user who is setting up his account or by a system administrator who defines access rights to a system depending on the level of permission granted. Clearly, if a user (primary or subordinate) is associated with a particular policy, the user is held to the rules of that policy.

In re claim 26 Bianco shows in figures 1-34 and related text, execution commands for accessing stored electronic data include permitting the user to access any of the following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections, electronic filing for taxes; privileges for permission to write checks, driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating report accounts, and; restricted portions of corporate intranet databases (column 2, lines 18-26).

In re claim 30 Bianco shows in figures 1-34 and related text, accessing electronic data comprises accessing any of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content, and; server-based computer software programs and hardware drivers (column 2, lines 1-18; column1, lines 8-13).

In re claim 31 Bianco shows in figures 1-34 and related text, at least one rule module further comprises any of the following: at least one pattern data associated with at least two execution commands; at least one execution command associated with at least two pattern data (column 18, lines 8-17).

In re claim 32 Bianco shows in figures 1-34 and related text, activation of an internet-connected device further comprises activating any of the following

devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; and electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; a digital audio player (column 1, lines 8-22)

In re claim 33 Bianco shows in figures 1-34 and related text, the automated intelligent agent for electronic data search and retrieval further comprises conducting periodic, user-customized on-line retrievals for any of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; faxes (column 12, lines 12-15).

In re claim 36 Bianco shows, in figures 1-34 and related text, invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission (column 54, lines 14-19).

In re claim 37 Bianco shows, in figures 1-34 and related text, the processing of electronic transmissions further comprises execution commands, which filter the access, and presentation of data when the user is subordinated user (column 49, lines 39-65).

In re claim 39 Bianco shows, in figures 1-34 and related text, execution commands for accessing stored electronic data include permitting the user to access any of the following: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes;

privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products; credit-rating and credit report accounts; restricted portions of corporate intranet databases (column 20, lines 17-32).

In re claim 41 Bianco shows, in figures 1-34 and related text, accessing membership benefits further comprises any of the following: validating a user's eligibility to rent videos under their prepaid membership; validating a user's eligibility to access an Internet web site; validating a user's eligibility to enter a real-time internet chat room with other people on-line (column 1, lines 8-33).

In re claim 43 Bianco shows in figures 1-34 and related text, any of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; server-based computer software programs and hardware drivers (column 20, lines 17-33).

In re claim 44 Bianco shows in figures 1-34 and related text, at least one rule module further comprises any of the following: at least one pattern data associated with at least two execution commands; at least one execution command associated with at least two pattern data (column 18, lines 8-17).

In re claim 45 Bianco shows in figures 1-34 and related text, activation of an internet-connected device further comprises activating any of the following devices: a wireless pager; a wireless telephone; a network computer; an exercise

machine; a television; and electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; a digital audio player (column 1, lines 8-22)

In re claim 46 Bianco shows in figures 1-34 and related text, the automated intelligent agent for electronic data search and retrieval further comprises conducting periodic, user-customized on-line retrievals for any of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; faxes (column 12, lines 12-15).

In re claim 49 Bianco shows, in figures 1-34 and related text, invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission (column 54, lines 14-19)

In re claim 50 Bianco shows, in figures 1-34 and related text, the processing of electronic transmissions further comprises execution commands which filter the access and presentation of data when the user is subordinated user (column 49, lines 39-65).

**Claim Rejections - 35 USC § 103**

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 27-29 and 34 are rejected under 35 U.S.C. 103(a) as being obvious over Bianco et al. (U.S. Patent No. 6,256,737).

In re claims 27, 28, 29, 34 the following activities: validating a user's health insurance benefits to permit admission to a hospital; validating a user's eligibility to rent videos under their prepaid membership; validating a user's eligibility to access an Internet web site; validating a user's eligibility to enter a real-time internet chat room with other people on-line; validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; validating a user's eligibility to board a vehicle of travel, are all known in the art to require a user's identity to be validated before information is released or access is permitted. The specification does not say that there is any critical modification to the invention in order to accommodate any of the above listed activities. Bianco shows, in figures 1-34 and related text, validating a user's eligibility to access an Internet web-site (column 2, lines 1-17; column 1, lines 8-12), which is recognized in the specification as equivalent to the other activities, listed above.

Therefore it would have been obvious to one of skill in the art at the time of the invention to do any of the above activities instead of validating a user's eligibility to access an Internet web-site for the explicit reasons discussed herein above.

14. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 14 above, and further in view of Herz (U.S. Patent No. 6,233,618).

In re claim 35 Bianco substantially discloses the invention as claimed but fails to show the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future. Herz shows, in an analogous art related to identification of customized electronic desirable objects in electronic media while ensuring the privacy of a user, in figures 1-16 and related text, the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future (column 7, lines 22-35). It would have been obvious to one of skill in the art at the time of the invention to replace the

execution command of Bianco with the automated intelligent agent of Herz because, for reasons of confidentiality and privacy, a user may not want to make public his personal purchasing patterns thus a trustworthy method of user authentication is required prior to allowing the user to access his profile (Herz, column 5, lines 20-52).

15. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 13 above, and further in view of Shannon (U.S. Patent No. 6,233,618).

In re claim 38 Bianco substantially discloses the invention as claimed but fails to show the filter governs subordinated access to any of the following: Internet web sites with adult content; internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user. Shannon shows, in an analogous art related to an access control technique that allows an administrator to limit a subordinate's access to information content on the Internet, in figures 1- 4 and related text, any of the following: Internet web sites with adult content; internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user (column 2, lines 43-52). It would have been obvious to one of skill in the art at the time of the invention to replace the filtered

content of Bianco with the filtered content of Shannon because restricted access may be useful in the home to deny access to objectionable web page material requested by children (Shannon, column 1, lines 47-67).

16. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 39 above, and further in view of Stock et al. (U.S. Patent No. 6,011,858).

In re claim 40 Bianco substantially discloses the invention as claimed but fails to show accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital. Stock et al. shows, in an analogous art related to biometric authentication of identity, in figures 1-10 and related text, accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital (column 7, lines 11-28). It would have been obvious to one of skill in the art at the time of the invention to replace the stored electronic data of Bianco with the insurance data a Stock et al. because conventional methods of verifying insurance, such as memory cards, are subject to fraud (column 1, line 50 – column 2, line 27).

17. Claims 42 & 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 39 above, and further in view of Mann et al. (U.S. Patent No. 6,119,096).

In re claim 42 Bianco substantially discloses the invention as claimed but fails to show any of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; validating a user's eligibility to board a vehicle of travel. Mann et al. shows, in an analogous art related to biometric access control the events, tourist attractions and transit systems, in figures 1-9 and related text, any of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; validating a user's eligibility to board a vehicle of travel (column 4, lines 34-47). It would have been obvious to one of skill in the art at the time of the invention to replace the stored electronic data of Bianco with the membership data of Mann et al. because conventional event "tickets" are subject to resale and scalping (Mann et al., column 1, lines 46-59).

In re claim 47 Mann et al shows, in figures 1-9 and related text, the vehicle of travel further comprises any of the following; a train; a boat; a bus (column 12, lines 45-53).

18. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 46 above, and further in view of Herz (U.S. Patent No. 6,233,618).

In re claim 48 Bianco substantially discloses the invention as claimed but fails to show the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future. Herz shows, in an analogous art related to identification of customized electronic desirable objects in electronic media while ensuring the privacy of a user, in figures 1-16 and related text, the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future (column 7, lines 22-35). It would have been obvious to one of skill in the art at the time of the invention to replace the execution command of Bianco with the automated intelligent agent of Herz because, for reasons of confidentiality and privacy, a user may not want to make public his personal purchasing patterns thus a trustworthy method of user

Art Unit: 3621

authentication is required prior to allowing the user to access his profile (Herz, column 5, lines 20-52).

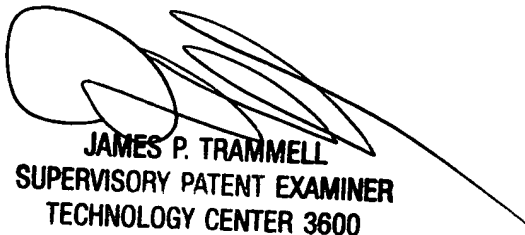
19. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco as applied to claim 50 above, and further in view of Shannon (U.S. Patent No. 6,233,618).

In re claim 51 Bianco substantially discloses the invention as claimed but fails to show the filter governs subordinated access to any of the following: Internet web sites with adult content; internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user. Shannon shows, in an analogous art related to an access control technique that allows an administrator to limit a subordinate's access to information content on the Internet, in figures 1- 4 and related text, any of the following: Internet web sites with adult content; internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" to the subordinated user during a particular on-line session, as pre-determined by the primary user (column 2, lines 43-52). It would have been obvious to one of skill in the art at the time of the invention to replace the filtered content of Bianco with the filtered content of Shannon because restricted access may be useful in the home to deny access to objectionable web page material requested by children (Shannon, column 1, lines 47-67).

**Conclusion**

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

  
JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **James A. Reagan** whose telephone number is **(703) 306-9131**. The examiner can normally be reached on Monday-Friday, 9:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **James Trammell** can be reached at (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the **Receptionist** whose telephone number is **(703) 305-3900**.

Any response to this action should be mailed to:

***Commissioner of Patents and Trademarks***

**Washington, D.C. 20231**

or faxed to:

**(703) 305-7687** [Official communications; including  
After Final communications labeled "Box AF"]

**(703) 308-1396** [Informal/Draft communications, labeled  
"PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7<sup>th</sup> floor receptionist.

JAR

03 December 2002

  
**JAMES P. TRAMMELL**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 3600**